CIBERSEGURANÇA: UM RELATO DE EXPERIÊNCIA SOBRE PROJETO PAUTADO NO MODELO ADDIE EM UM CENTRO ESTADUAL DE EDUCAÇÃO PROFISSIONAL

João Pedro Mendes de Oliveira, Francisca Ocilma Mendes Monteiro
joaopedromendesofc@gmail.com, ocilma.monteiro@ifpi.edu.br

Descrição Geral

A constante evolução tecnológica trouxe melhorias significativas à sociedade, mas acompanhada de desafios, como a vulnerabilidade digital por falta de conhecimento técnico. Este trabalho relata a experiência do projeto "**Aprendendo a se Proteger na Era Digital**", fundamentado no modelo **ADDIE** (*Analysis, Design, Development, Implementation, Evaluation*). A aplicação ocorreu com estudantes do Ensino Médio Integrado ao curso Técnico em Informática em um Centro Estadual de Educação Profissional, em Teresina-PI.

O objetivo central foi capacitar os discentes em práticas de cibersegurança, alinhando conceitos teóricos à realidade cotidiana para conscientização sobre os riscos digitais. Foram abordados temas como privacidade *online*, ameaças cibernéticas e medidas preventivas. A metodologia adotada foi a pesquisa-ação de natureza qualitativa, utilizando observações participantes, diários de campo e questionários. Os resultados apontaram um aumento expressivo no engajamento e na adoção de boas práticas, evidenciando a eficácia do modelo instrucional.

Objetivos

O planejamento do projeto seguiu as cinco etapas do modelo ADDIE. Os objetivos específicos e os alcances obtidos estão detalhados no Quadro 1:

Quadro 1- Matriz de Objetivos e Resultados Alcançados

Objetivo	Resposta Alcançada	Metodologia de Alcance
Planejar o projeto via modelo ADDIE	Estrutura pedagógica completa.	Desenvolvimento sistemático das 5 fases do modelo.
Desenvolver atividades sobre crimes digitais	Compreensão prática de conceitos abstratos	Oficinas de resolução de problemas e estudos de caso.
Ensinar sobre *phishing* e	Adoção de novos	Demonstração de técnicas de ataque

Objetivo	Resposta Alcançada	Metodologia de Alcance
senhas seguras	hábitos de proteção.	e critérios de senhas.
Apresentar ferramentas de auxílio	Familiaridade com recursos de verificação	Uso do *Have I Been Pwned* e mapas de ataques em tempo real.
Avaliar a mudança de comportamento	Conscientização e mudança de postura.	Aplicação de questionário pós-intervenção e análise.

Fonte: Elaborado pelos autores (2025).

Habilidades Trabalhadas

O projeto foi desenhado em conformidade com a Base Nacional Comum Curricular (BNCC) e seu complemento em Computação, focando no uso consciente, seguro e responsável das tecnologias. As atividades mobilizaram as seguintes competências e habilidades:

- **Conceitos Técnicos -** *Phishing* (engano), Engenharia Social (manipulação), *Malwares* (*softwares* maliciosos);
- **EM13CO08 -** Entender como mudanças na tecnologia afetam a segurança, incluindo novas maneiras de preservar sua privacidade e dados pessoais on-line, reportando suspeitas e buscando ajuda em situações de risco.
- **EM13CO10** - Conhecer os fundamentos da Inteligência Artificial, comparando-a com a inteligência humana, analisando suas potencialidades, riscos e limites.
- **EM13CO14** - Avaliar a confiabilidade das informações encontradas em meio digital, investigando seus modos de construção e considerando a autoria, a estrutura e o propósito da mensagem.

Ao trabalhar a **EM13CO08**, o foco transcendeu o uso instrumental, buscando desenvolver a capacidade crítica de analisar vulnerabilidades, tornando o aluno um agente ativo em sua própria segurança digital.

Materiais Utilizados

Os materiais e recursos utilizados para a realização do projeto foram: laboratório com computadores e acesso à internet; quadro branco e pincéis; projetor e material de apoio (slides); apostila "*Aprendendo a se Proteger na Era Digita*l" no formato digital.

Metodologia e Sequência Didática

Seguindo as premissas de Filatro (2008), o projeto dividiu-se em:

1. **Análise:** Identificação das necessidades de conhecimento do público-alvo.
2. **Design**: Elaboração do plano de ensino e seleção de conteúdos.
3. **Desenvolvimento:** Produção da apostila e dos roteiros das oficinas.
4. **Implementação:** Execução das aulas e práticas laborais.
5. **Avaliação:** Análise qualitativa e quantitativa da aprendizagem.

As aulas adotaram uma abordagem teórico-prática, por meio da utilização do material base, a apostila 'Aprendendo a se Proteger na Era Digital', alinhada aos princípios da pesquisa-ação e da aprendizagem ativa.

Cada encontro iniciava com uma exposição conceitual relacionada à cibersegurança, como: crimes digitais, *phishing*, uso de senhas seguras e ameaças presentes no ambiente digital. Foram realizadas demonstrações práticas e atividades orientadas, nas quais os alunos puderam aplicar os conceitos discutidos, por meio da análise de exemplos reais, simulações de situações de risco e utilização de ferramentas online voltadas à segurança da informação, como, por exemplo, o site *Have I Been Pwned*, que apresenta se seu email foi vítima de um vazamento de dados pela internet e o *Cybermap* da *Kaspersky* que apresenta os ataques digitais em tempo real pelo globo terrestre. Essas atividades tiveram como objetivo promover a participação ativa dos estudantes e estimular o desenvolvimento do pensamento crítico em relação aos riscos digitais.

Ao final de cada aula, promovia-se um momento de discussão coletiva, permitindo que os alunos compartilhassem suas percepções, soluções e dificuldades encontradas durante as atividades. Esse espaço de diálogo contribuiu para a consolidação dos conhecimentos e para a reflexão sobre práticas seguras no uso das tecnologias digitais.

Os dados foram coletados por meio de observação direta realizada em sala de aula, registradas em diários de campo (Falkembach, 1987). O registro de observações e reflexões após cada aula, visa compreender o nível de conhecimento dos alunos em relação ao conteúdo ministrado e documentar o desenvolvimento da turma.

Outro instrumento utilizado foi um questionário composto por 10 perguntas que abordou os principais temas apresentados e discutidos durante o projeto visando analisar o desenvolvimento e identificar avanços nos conhecimentos adquiridos.

Avaliação

A avaliação dos resultados foi realizada por meio de diários de campo, observações em sala de aula como também a aplicação de um questionário ao final do

projeto. Todo o projeto teve uma carga horária de 40 horas, divididas em 20 encontros, com duração de 2 horas cada.

Os resultados indicaram que 85% dos alunos demonstraram uma melhoria significativa no conhecimento sobre boas práticas de segurança digital, como o uso de senhas fortes, autenticação de dois fatores, e os riscos de navegação em sites não seguros; 75% dos alunos relataram ter adotado novas práticas de segurança após as atividades realizadas, como o uso de antivírus, atualizações constantes nos aparelhos móveis e a escolha mais criteriosa na composição de suas senhas; e 70% dos alunos estavam conscientes da importância da cibersegurança no ambiente digital e sua relação direta com a proteção de dados pessoais e financeiros. Essas respostas refletem a eficácia do projeto na transmissão de conceitos essenciais sobre segurança no mundo digital.

Quadro 2 - Desempenho no Questionário Final (N=32)

Questão	**Eixo Temático**	**Acertos** (Média)	**Erros** (Média)
1-2	Tipos de hackers	24	8
3-4	Fundamentos de rede	24	8
5-6	Vulnerabilidades e características	19,5	12,5
7-8	Boas práticas e mitigação	24,5	7,5
9-10	Protegendo dispositivos móveis	29	3

Fonte: Elaborado pelos autores (2024).

Conclusão

A aplicação do modelo ADDIE mostrou-se eficaz para estruturar o ensino de cibersegurança, resultando em maior engajamento e assimilação de conteúdos complexos. O projeto de implementação sobre cibersegurança demonstrou ser uma iniciativa relevante para enfrentar os desafios de um mundo cada vez mais digital e exposto a ameaças cibernéticas. De modo geral, a proposta alcançou os objetivos propostos, confirmando a hipótese de que a aplicação do projeto contribuiu significativamente para a ampliação do entendimento dos alunos e para a adoção de práticas mais seguras no ambiente digital. A abordagem pedagógica adotada, baseada no modelo ADDIE, favoreceu um aprendizado mais dinâmico e contextualizado. Observou-se que os alunos apresentaram maior engajamento durante as atividades práticas,

especialmente as que envolviam simulações de ataques cibernéticos e situações próximas à sua realidade digital cotidiana. Essas estratégias mostraram-se eficazes para despertar o interesse dos estudantes e facilitar a assimilação dos conteúdos relacionados à segurança da informação.

Por outro lado, identificou-se que alguns conceitos mais abstratos, como determinados tipos de ameaças digitais e estratégias de proteção menos visíveis ao usuário comum, tornaram a compreensão mais desafiadora por parte dos alunos, exigindo uma maior mediação pedagógica por parte do professor. Essa constatação sugere a necessidade de ampliar o uso de exemplos concretos, estudos de caso e mais recursos visuais em futuros projetos.

A análise dos dados obtidos por meio dos instrumentos utilizados evidenciou avanços no entendimento dos alunos sobre segurança digital, uma conscientização maior acerca do uso das tecnologias e da importância da proteção de dados pessoais. Nesse sentido, a sequência didática dos encontros não se limitaram à transmissão de conhecimentos técnicos, mas contribuíram para a formação de uma postura mais crítica e responsável frente ao ambiente digital.

Por fim, a experiência reforça a importância de iniciativas educacionais alinhadas às demandas do mundo contemporâneo, nas quais a cibersegurança deve ser tratada como uma prioridade. A continuidade e o aprimoramento de projetos dessa natureza são fundamentais para a consolidação de uma cultura de segurança digital e para a formação de estudantes capazes de atuar como multiplicadores do conhecimento e de práticas seguras em seus contextos sociais.

Referências

FILATRO, A. **Design instrucional na prática**. São Paulo (SP): Pearson Education do Brasil, 2008.

FALKEMBACH, Elza Maria Fonseca. **Diário de campo: um instrumento de reflexão**. In: Contexto e Educação, nº 7, Juí: Inijuí, 1987.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de Metodologia Científica**. 5. ed. São Paulo: Atlas S.A., 2003.

STEINBERG, Joseph. **Cibersegurança para leigos**. Rio de Janeiro: Alta Books, 2020.

BRASIL. Ministério da Educação. Conselho Nacional de Educação. Câmara de Educação Básica. **Parecer CNE/CEB nº 2/2022, de 17 de fevereiro de 2022**. Normas sobre Computação na Educação Básica: complemento à Base Nacional Comum Curricular (BNCC). Brasília, DF: MEC/CNE, 2022. Disponível em: https://www.gov.br/mec/pt-br/cne/pdf/pareceres-do-cne/ceb/2022/pceb002_22.pdf. Acesso em: jul. 2025.